INFORMATION SYSTEMS AUDITING REQUIREMENTS

John W. Lainhart IV
Inspector General
U.S. House of Representatives
485 Ford House Office Building
Washington, D.C. 20515-9990

Not a new direction or challenge for information systems security, but a direction often not pursued and a challenge often not addressed, information systems auditing is critically required in today's information systems intensive environment. It is required to ensure that our mission critical or lifeblood systems are designed and continue to be maintained with confidentiality, integrity, and availability foremost in mind. In addition, information systems auditing is required by professional auditing standards when information systems are involved in the area being audited. To assist in this effort, a new set of standards, *CobiT* (Control Objectives for Information and Related Technology) was recently issued which contains both information technology (IT) control objectives, for management and users, and information systems audit guidelines, for auditors.

Standards Relating to Audits Involving Information Systems

The American Institute of Certified Public Accountants (AICPA) in several *Statements on Auditing Standards* (SASs), Institute of Internal Auditors Association (IIA) in its *Standards for the Professional Practice of Internal Auditing*, Information Systems Audit and Control Association (ISACA) in its *General Standards for Information Systems Auditors* and *Statements on Information Systems Auditing Standards*, and U.S. General Accounting Office (GAO) in its *Government Auditing Standards* and *Title 2, Accounting*, have all taken essentially the same position concerning audits involving information systems. The bottom line is that when an information system is an important and integral part of the operations being audited, the audit should include an appropriate examination of the system to provide reasonable assurance that the information produced by the system is valid and reliable (relevant, accurate, and complete, in light of its intended use).

Specifically, GAO's *Government Auditing Standards* states that "auditors should obtain sufficient, competent, and relevant evidence that computer processed data are valid and reliable when those data are significant to the auditors' findings." The *Government Auditing Standards* goes on to state that "when the reliability of a computer-based system is the primary objective of the audit, the auditors should conduct a review of the system's general and application controls." Furthermore, in its *Appendix III, Accounting System Standards, Chapter 4, Accounting System Development and Modification*, of *Title 2*, GAO states that Offices of Inspectors General (OIGs) are an important factor contributing to successful accounting and financial management system development and modification efforts. GAO indicates that while normally not a member of the project team, auditor involvement is needed in reviewing and evaluating these development and modification efforts.

CobiT -- Control Objectives for Information and Related Technology

In order to facilitate this review of information systems, ISACA recently issued *CobiT*. It was developed as a generally applicable and accepted international standard for good practices for IT controls. *CobiT* is based on ISACA's existing *Control Objectives*, enhanced with existing and emerging international technical, professional, regulatory, and industry-specific standards. It was written for three specific audiences -- management, users, and auditors. By using this document, management will be able to review the organization's information systems to make IT investment decisions, balance risks and controls, and benchmark its existing and future IT environments. Users will be able to obtain assurance on the security and control of products they acquire (internally or externally). Finally, auditors will be able to substantiate internal control opinions and identify needed minimum controls for management.

CobiT identifies 4 domains with 32 IT processes which form the *Framework* for from 5 to 25 detailed *Control Objectives.* The first domain, planning and organization, covers strategy and tactics and concerns the identification of the way IT can best contribute to the achievement of business objectives. It also emphasizes that a proper organization, as well as technological infrastructure, must be in place. The second domain, acquisition and implementation, recognizes that to realize the IT strategy, IT solutions need to be identified, developed, or acquired as well as implemented and integrated into the business process. It also addresses changes to and maintenance of existing systems. The third domain, delivery and support, is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. This domain also includes the actual processing of data by application systems. The final domain, monitoring, recognizes that all IT processes need to be regularly assessed over time for their quality and compliance with control requirements.

In addition to the domains, processes, and control objectives which are used by management, users, and auditors, *CobiT* provides detailed *Audit Guidelines* for auditors to follow in performing information systems audits -- thereby, meeting their information systems auditing requirements! Thus, the *Audit Guidelines* provide a complementary tool to enable the easy application of the *Framework* and *Control Objectives* within audit activities. *CobiT* states that the objectives of auditing are to: (1) provide management with reasonable assurance that control objectives are being met; (2) where there are significant control weaknesses, to substantiate the resulting risks; and (3) advise management on corrective actions needed (ones needed at a minimum, and ones that are cost beneficial). *CobiT* goes on to state that information systems are audited by: (1) **obtaining an understanding** of business requirements related risks, and relevant control measures; (2) **evaluating the appropriateness** of stated controls; (3) **assessing compliance** by testing whether the stated controls are working as prescribed, consistently and continuously; and (4) **substantiating the risk** of control objectives not being met by using analytical techniques and/or consulting alternative sources.

Conclusion

Clearly, information systems auditing is mandated by an abundance of specific professional standards -- from both public and private accounting and auditing organizations. But even more important is the need of our organizations for increased quality, decreased delivery time, and continuous service level improvements. All these aspects must be achieved within tighter cost constraints, with fewer resources. At the same time, assets of the organization must be adequately safeguarded, and for many organizations, information and the technology that supports it represent the organization's most valuable assets. Thus, it just makes good sense to aggressively audit information systems -- both those that are operational (general and application systems) and those that are under development or modification.